Décomposition d'un groupe commutatif fini

(Dany-Jack MERCIER, 1979)

I Définition d'un p-groupe

Def Soit G un groupe. On dit que G est un p-groupe si son cardinal est une puissance de p ($p \in \mathcal{P}$).

Th Soit G un groupe commutatif fini.
Alors $G = p\text{-groupe} \iff \{ \forall x \in G\ \exists \alpha \in \mathbb{N}\ /\ \omega(x) = p^\alpha \}$

preuve : • Supposons que $\forall x \in G\ \omega(x) = p^\alpha$. On fait une récurrence sur le cardi de G. En notation additive :
→ Pour $G = \{0\}$, c'est évident
→ Soit G de cardinal n. Soit $x \in G$, $x \neq 0$. Notons $H = \langle x \rangle$. C'est un groupe cyclique d'ordre p^k. Mais $\# G = \# H \cdot \# G/H$ et G/H, groupe commutatif, vérifie $\forall \dot{x} \in G/H\ \exists \alpha\ /\ p^\alpha \dot{x} = \dot{0}$. De plus $\# G/H < \# G$. L'hypothèse de récurrence s'applique : $\# G/H = p^\beta$. Comme $\# H = p^k$, on trouve que $\# G = p^{\beta + k}$ cqfd
• Inversement, si G est un p-groupe, $\# G = p^k$ et tout élément x de G engendre $\langle x \rangle$ d'ordre $p^\alpha \mid p^k$. Par suite $\omega(x) = p^\alpha$.

II Décomposition en p-groupes (ou "composantes p-primaires")

Th Soit G un groupe commutatif fini d'ordre $n = p_1^{r_1} \cdots p_k^{r_k} = q_1 \cdots q_k$
Posons $G(p_i) = \{ x \in G\ /\ q_i x = 0 \}$
$G(p_i)$ est un p_i-groupe et :

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

Il est clair que $G(p_i)$ est un groupe, et que $\forall x \in G(p_i)\quad \omega(x) \mid p_i^{r_i} \Rightarrow \omega(x) = p_i^{\ldots}$
donc $G(p_i) = p_i$-groupe.
Montrons la somme directe :
* $\forall x \in G\quad \exists x_i \in G(p_i)\ /\ x = x_1 + \cdots + x_k$?
Il est clair que $\Delta\left(\frac{n}{q_1}, \frac{n}{q_2}, \ldots, \frac{n}{q_k}\right) = 1 \iff \sum_{i=1}^{k} m_i \frac{n}{q_i} = 1$ (Bezout)

$$\text{Donc } x = \underbrace{m_1 \frac{n}{q_1} x}_{\in G(p_1)} + \cdots + \underbrace{m_k \frac{n}{q_k} x}_{\in G(p_k)}$$

Donc $G = G(p_1) + \cdots + G(p_k)$
* $\forall j \in [1, k]\quad G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j) = \{0\}$?
Soit $x \in G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j)$ où $j \in [1, k]$
Alors $q_j x = 0$ et $x = x_1 + \cdots + x_{j-1}$ où $x_i \in G(p_i) \iff q_i x_i = 0\quad \forall i$
Soit $s = \prod_{i=1}^{j-1} q_i$. On a $sx = 0$

q_j et s sont premiers entre eux ! donc $\lambda q_j + \mu s = 1 \Rightarrow x = \lambda q_j x + \mu s x$

CQFD

III Décomposition en p-groupes cycliques.

Enonçons tout d'abord :

Th 1 | Tout p-groupe commutatif G se décompose en groupes cycliques p-primaires,

$$G \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z} \qquad \alpha_1 \leq \dots \leq \alpha_s$$

De plus, la suite $(\alpha_1, \dots, \alpha_s)$ est unique.

Soit G un p-groupe commutatif. Enonçons 2 lemmes :

<u>lemme 1</u> : $\left.\begin{array}{l} b \in G \quad b \neq 0 \quad p^k b \neq 0 \\ \omega(p^k b) = p^m \end{array}\right\} \Rightarrow \omega(b) = p^{m+k}$

<u>lemme 2</u> : Soit $a_1 \in G$ $G_1 = \langle a_1 \rangle$ / $\# G_1 = p^{r_1} = \operatorname{Sup}\{\omega(x) / x \in G\}$

Soit $\dot{b} \in G/G_1$ tel que $\omega(\dot{b}) = p^r$. On pose $\pi_1 : G \to G/G_1$

Alors $\exists b$ / $\pi_1(b) = \dot{b}$ et $\omega(b) = p^r$.

<u>preuve lemme 1</u> : On a $\left\{\begin{array}{l} p^{m+k} b = 0 \\ p^{m+k-1} b = p^{m-1}(p^k b) \neq 0 \text{ car } \omega(p^k b) = p^m \quad (m \geq 1) \end{array}\right.$

donc $\omega(b) = p^{m+k}$

<u>preuve lemme 2</u> : Soit $b \in G$ tel que $\pi_1(b) = \bar{b}$. π_1 est un morphisme de groupes, donc il abaisse les ordres des éléments : $\omega(b) \geq p^r$, $\forall b \in \pi_1^{-1}(\bar{b})$. (*)

On a $p^r b \in G_1 \iff p^r b = n\, a_1$ où $0 \leq n < p^{r_1}$

$p^r b = p^k \mu a_1$ où $p \nmid \mu$ $(k < r_1)$

$\omega(p^k \mu a_1) = \dfrac{p^{r_1}}{\Delta(p^k\mu, p^{r_1})} = p^{r_1 - k}$ et $p^r b \neq 0 \underset{(\text{lemme } 1)}{\Longrightarrow} \omega(b) = p^{r + r_1 - k}$

Comme $p^{r_1} = \operatorname{Sup}\{\omega(x) / x \in G\}$ et que $\omega(b) = p^{r+r_1-k}$, on aura forcément l'inégalité : $r + r_1 - k \leq r_1 \iff r \leq k$

Par suite : $p^r b = p^k \mu a_1 \Rightarrow (b - p^{k-r}\mu a_1)p^r = 0 \Rightarrow \omega(b - p^{k-r}\mu a_1) = p^r$ (cf. (*))

On a qu'à prendre $b' = b - p^{k-r}\mu a_1 \in \pi^{-1}(\dot{b})$

<u>preuve du théorème</u> :

• <u>Existence de la décomposition</u>

$\# G = p^u$. On fait une récurrence sur u.

C'est vrai pour u=1. Soit G de cardinal $\# G = p^u$. Alors $\# G/G_1 = p^{u-r_1}$ et l'on peut appliquer l'hypothèse de récurrence :

$$G/G_1 = \bar{G}_2 \oplus \dots \oplus \bar{G}_s \quad \text{où } \bar{G}_i = \dot{a}_i \mathbb{Z} \quad \omega(\dot{a}_i) = p^{r_i}$$

(groupes cycliques primaires)

D'après le lemme 2 :

$$\exists a_i \in G \;/\; \pi(a_i) = \dot{a}_i \text{ et } \omega(a_i) = p^{r_i}$$

Posons $G_i = a_i\mathbb{Z} = \langle a_i \rangle$ et montrons que $G = G_1 \oplus \dots \oplus G_s$:

1) $G = G_1 + \dots + G_s$

En effet, $\forall x \in G$ $\dot{x} = m_2 \dot{a}_2 + \dots + m_s \dot{a}_s \iff x = \underbrace{m_1 a_1}_{\in G_1} + \dots + m_s a_s$.

2) Si $m_1 a_1 + \dots + m_s a_s = 0$ $\quad 0 \leq m_i < p^{r_i}$

alors $m_2 \dot{a}_2 + \dots + m_s \dot{a}_s = 0$ d'où $m_2 = \dots = m_s = 0$ et $m_1 a_1 = 0 \Rightarrow m_1 = 0$

Donc $G = G_1 \oplus \dots \oplus G_s$ $\quad G_i$ = groupe cycliques primaires d'ordre p^{α_i}

• <u>Unicité de la suite $(\alpha_1, \dots, \alpha_s)$</u>

On a $G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^t\mathbb{Z})^{m_t}$

Montrons que cette décomposition est unique.

$$G[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1}[p] \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_r}[p]$$

$$G[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times p(\mathbb{Z}/p^2\mathbb{Z})^{m_2} \times \dots \times p^{t-1}(\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

(où $G[p] = \{x \in G \,/\, px = 0\}$ = "p-groupe élémentaire de G" = groupe d'ordre p.)

Mais pour $h \leq k$ $\quad p^k(\mathbb{Z}/p^h\mathbb{Z}) = 0$. Donc :

$$p^k G \simeq p^k(\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times p^k(\mathbb{Z}/p^r\mathbb{Z})^{m_t}$$
$$\simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^r\mathbb{Z})^{m_t}$$

donc $p^k G \cap G[p] \simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^r\mathbb{Z})^{m_t}$ } ⊛ (1) je ne vois pas pour... ce juillet 96. cf Alternative page... qui n'utilise que p...

Comme, d'autre part $(p^k\mathbb{Z}/p^{i+1}\mathbb{Z}) \,/\, (p^i\mathbb{Z}/p^{i+1}\mathbb{Z}) \simeq p^k\mathbb{Z}/p^i\mathbb{Z}$

et comme, dans un groupe commutatif $(H \times H')/(K \times K') \simeq H/K \times H'/K'$
(cf. 2.12 bouvier), on obtient :

$$\underbrace{p^k G \cap G[p] \,/\, p^{k+1}G \cap G[p]}_{} \simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \simeq (\mathbb{Z}/p\mathbb{Z})^{m_{k+1}}$$

p-groupe élémentaire. C'est donc un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$.
On voit ici qu'il est de dimension m_{k+1}. Ainsi :

$$m_{k+1} = \dim_{\mathbb{Z}/p\mathbb{Z}} \frac{p^k G \cap G[p]}{p^{k+1} G \cap G[p]}$$ qui ne dépend que de k et de G.

m_{k+1} est donc indépendant de la décomposition choisie.

Ainsi : $G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_t} \simeq (\mathbb{Z}/p\mathbb{Z})^{m'_1} \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m'_{t'}}$

$$\Downarrow \qquad (t \leq t')$$

$$m_1 = m'_1 \; ; \dots ; \; m_t = m'_t$$

Un argument de "cardinal" montre que $p^{m_1 + \dots + t m_t} = p^{m'_1 + \dots + t' m'_{t'}}$
donc que $(t+1) m'_{t+1} + \dots + t' m'_{t'} = 0 \Rightarrow m'_{t+1} = \dots = m'_{t'} = 0$.

CQFD

Th2 | Soit G un groupe fini commutatif d'ordre $n = p_1^{r_1} \dots p_k^{r_k}$
G est décomposable en groupes cycliques primaires, et l'on a :

$$G \simeq \mathbb{Z}/p_1^{\alpha_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{\alpha_{12}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{\alpha_{1n_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{k1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{kn_k}}\mathbb{Z}$$

où $\begin{cases} p_1 < p_2 < \dots < p_k \\ \alpha_{i1} \leq \dots \leq \alpha_{in_i} \end{cases}$

La suite $(p_1^{\alpha_{11}}, \dots, p_1^{\alpha_{1n_1}}, \dots, p_k^{\alpha_{k1}}, \dots, p_k^{\alpha_{kn_k}})$ est parfaitement déterminé. Il se nomme "<u>le type de G</u>".

Ce théorème nous révèle la structure de tout groupe commutatif fini.
Il se démontre en utilisant le théorème de décomposition en groupes primaires

⊛ <u>Alternative</u> : Pourquoi parler de $G[p]$? Certains résultats restent à justifier ce-dernier au ⊛, alors utilisons seulement :

$$p^kG \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \left(p^k\mathbb{Z}/p^{k+2}\mathbb{Z}\right)^{m_{k+2}} \times \dots \times \left(p^k\mathbb{Z}/p^t\mathbb{Z}\right)^{m_r}$$

pour obtenir

$$p^kG/p^{k+1}G \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+2}} \times \dots \times \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_r}$$

$$\simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m_{k+1}+\dots+m_r}$$

C'est encore un e.v. sur le corps $\mathbb{Z}/p\mathbb{Z} \doteq \mathbb{F}_p$, soit :

$$m_{k+1}+\dots+m_t = \dim_{\mathbb{F}_p}\left(p^kG/p^{k+1}G\right)$$

Cette dernière dim. est dépendante de G et de k uniquement, et l'égalité précédente permet d'obtenir successivement $m_r, m_{r-1}, \dots, m_1$ à partir de ces dimensions : l'unicité de $m_1, m_2, \dots, m_r$ est donc établie. (…)

Pour conclure, considérons encore :

$$G \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m_1} \times \dots \times \left(\mathbb{Z}/p^r\mathbb{Z}\right)^{m_r} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m'_1} \times \dots \times \left(\mathbb{Z}/p^{t'}\mathbb{Z}\right)^{m'_{t'}}$$

On peut toujours supposer que $t=t'$ quitte à rajouter des m_i nuls.

Vu ce qui précède, on aura :

$$\begin{cases} m_t = m'_t \\ \dots \\ m_1 = m'_1 \end{cases}$$

CQFD

$G = G(p_1) \oplus \ldots \oplus G(p_k)$ (cf paragraphe II)
et en utilisant le Th 1 ci-dessus :

$$G(p_i) \simeq \mathbb{Z}/_{p_i^{\alpha_{i1}}} \times \ldots \times \mathbb{Z}/_{p_i^{\alpha_{in_i}}}$$

L'unicité de la décomposition $(p_1^{\alpha_{11}}, \ldots, p_k^{\alpha_{kn_k}})$, qui détermine le type de G, est dû :

1) à l'unicité de la suite du th. 1 : $(p_i^{\alpha_{i1}}, \ldots, p_k^{\alpha_{kn_k}})$ est unique.

2) à la remarque suivante : $G = G(p_1) \oplus \ldots \oplus G(p_k)$
Si G_i est p_i-primaire cyclique, alors $\forall x \in G_i \quad p_i^{\# G_i} x = 0$, donc $x \in G(p_i) = \{x \in G \,/\, p_i^{n_i} x = 0\}$. Ainsi $G_i \subset G(p_i)$

CQFD

Application :

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de type $(2, 2)$

$\mathbb{Z}/4\mathbb{Z}$ est de type (2^2)

$G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$ est de type $(2^3, 2^4, 3^2, 5^3)$

Remarque : G est d'ordre $2^7 \times 3^2 \times 5^3 = 14400$ et de type $(2^3, 2^4, 3^2, 5^3$
Le type $(2^3, 2^4, 3^2, 5^3)$ ne doit pas être confondu avec le k-uplet $(p_1^{n_1}, \ldots, p_k^{n_k})$ de la décomposition de n en facteurs premiers.

Toutefois, puisque $n = \# G = \prod_{\substack{i=1,k \\ j=1,n_i}} \#\left(\mathbb{Z}/_{p_i^{\alpha_{ij}}}\right)$, on trouve que :

$$\begin{cases} n_1 = \sum_{j=1}^{n_1} \alpha_{1j} \\ \text{- - - -} \\ n_k = \sum_{j=1}^{n_k} \alpha_{kj} \end{cases} \quad \text{où } n = p_1^{n_1} \ldots p_k^{n_k}$$

Co | Deux groupes abéliens finis sont isomorphes ssi ils ont même type

preuve : Si G et G' ont même type, il est clair qu'ils sont isomorphes.
Inversement si $G \simeq G'$, soit $G = \bigoplus_{i=1}^{m} \Gamma_i$ et $G' = \bigoplus_{i=1}^{m'} \Gamma_i'$ les décompositions de G et G' en groupes cycliques primaires.
$\Phi : G \xrightarrow{\sim} G'$. Alors $\bigoplus_{i=1}^{m} \Phi(\Gamma_i)$ est une décomposition de G' en groupes cycliques primaires.
D'après l'unicité des types, $m = m'$ et les types de G et de G' sont les m̂.